Annual Conference of Postgraduate Studies and Scientific Research (Basic and Engineering Studies Board)
17-20 February 2012, Friendship Hall, Khartoum

Evaluating the Impact of Encryption on Voice over Internet Protocol (VoIP) Systems

Sulafa Khaled Talha and Bazara I. A. Barry

Faculty of Mathematical Sciences, University of Khartoum

Abstract: Securing computer systems has become of vital importance especially with the sophistication and advancement of attacking tools and techniques. Therefore, it is critical to apply security mechanisms that are capable of protecting systems in a way that ensures and provides major security services. However, providing a system with security services comes at the expense of system performance. The resource-intensive nature of effective security mechanisms may have a negative impact on certain aspects of system performance.

A major security service that is required in computer networks and information systems is confidentiality which ensures that transmitted data are protected from unauthorized disclosure. Encryption is the security mechanism that is used to provide confidentiality. Prior to transmitting sensitive data over an information channel, encryption algorithms transforms data into a form that is not readily intelligible. On the side of the receiver, a decryption operation takes place to recover the original form of the sent data. Clearly, encryption and decryption operations have their impact on the performance of the system.

This study investigates the impact of providing confidentiality services on the performance of systems. The study takes Voice over Internet Protocol (VoIP) systems - which are used to make telephone calls over the Internet - as an example of systems that are greatly affected by performance degradation. The study measures how key VoIP performance parameters are impacted when certain encryption algorithms are implemented, and whether that impact falls within the tolerable levels.

Keywords: VoIP, Performance, Encryption, SIP

المستخلص: أصبح تأمين أنظمة الحاسوب من الأهمية بمكان لا سيما مع تعقيد و تقدم وسائل و أدوات المهاجمين. لذا صار ضرورياً أن تُطبق آليات لها القدرة على حماية تلك النظم بطريقة تضمن توفير خدمات التأمين الأساسية. غني عن الذكر أن توفير خدمات التأمين الأساسية يأتي على حساب أداء النظام في كثير من الأحيان. تعتبر خدمة الخصوصية من أهم خدمات التأمين فهي تحمي البيانات المنقولة من الإطلاع غير المأذون به. يبرز التشفير باعتباره الألية التي تستخدمها خدمة الخصوصية، فقبل إرسال البيانات الحساسة تقوم خوارزميات التشفير بتحويل البيانات لشكل لاتمكن قراءته. على جانب المستقبل تستخدم خوارزميات فك التشفير

لإعادة البيانات لطبيعتها. من الجلي أن عمليات التشفير و فكه تترك أثراً على أداء النظام. تناقش هذه الورقة أثر توفير خدمة الخصوصية على أداء النظام، حيث تأخذ كمثال نظم نقل الصوت على بروتوكول الإنترنت . التي تستخدم لإجراء المكالمات الهاتفية على شبكة الإنترنت . باعتبارها تتأثر بشدة بانخفاض الأداء. تقيس الورقة مدى تأثر محددات الأداء الأساسية في نظم نقل الصوت على الإنترنت باستخدام خوارزميات تشفير معينة، و إذا ما كان هذا التأثر واقعاً ضمن الحدود المسموح بها.

الكلمات المفتاحية: الصوت على بروتوكول الإنترنت، الأداء، التشفير، بروتوكول بدء الجلسة

I. INTRODUCTION

Several protocols and mechanisms aim to provide the various security services in computer systems due to the sophistication and advancement of attacking tools and techniques. Three basic security services important to computer systems are confidentiality, integrity, and availability. These services provide protection against malicious software (malware), spyware, spam and phishing attacks.

Data confidentiality:

Confidentiality refers to limiting information access and disclosure to authorized users and preventing access by or disclosure to unauthorized ones.

Underpinning the goal of confidentiality are authentication methods like user-IDs and passwords, which uniquely identify a data system's users, and supporting control methods that limit each identified user's access to the data system's resources.

Confidentiality is related to the broader concept of data privacy. It limits access to individuals' personal information.

Data integrity*:*

Integrity refers to the trustworthiness of information resources. It insures that data have not been changed inappropriately, whether by accident or deliberately malign activity. It also insures that the data actually came from the actual sender, rather than an imposter.

On a more restrictive view, however, integrity of an information system includes only preservation without corruption of whatever was transmitted or entered into the system, right or wrong.

Data availability:

Availability refers to the availability of information resources. An information system that is not available when it is needed is at least as bad as none at all. It becomes critical when the organization has become on a functioning computer and communications infrastructure.
Availability, like other aspects of security, may be affected by purely technical issues, natural phenomena, or human causes.
Adding such security mechanisms to computer systems does not come cheaply, as these mechanisms have impacts on system performance.

Voice over Internet Protocol (VoIP) is a technology that is used to transmit voice conversations using the Internet Protocol (IP) over a packet-switched network. VoIP is based on computer networks, so it is vulnerable to all security attacks that target computer networks. Another issue that concerns VoIP system designers is performance. A VoIP conversation with lengthy end-to-end delay or jitter is unacceptable to users.

To protect the information transmitted over the network encryption algorithms or cryptographic functions can be applied to the packet payload. This can affect the end to end QoS (quality of service) experienced by the user. The stronger the encryption algorithm the greater the level of security and the greater the corresponding effect on the performance of the VoIP.

This study investigates the impact of providing confidentiality on the performance of systems. The study takes Voice over Internet Protocol (VoIP) systems as an example of systems that are greatly affected by performance degradation.
Three parameters are chosen to measure VoIP performance, which are end-to-end delay, jitter and packet loss. AES encryption algorithm will be used to secure the VoIP calls.
The study measures how key VoIP performance parameters are impacted when AES encryption is implemented, and whether that impact falls within the tolerable levels.
This paper gives background about VoIP and encryption in the second section. The third section discusses VoIP performance parameters and how they are impacted by encryption. The fourth section sheds light on our experimental case study and the fifth section demonstrates the results. The sixth section concludes the paper.

II. BACKGROUND

VoIP is a technology used to transmit voice conversations using the IP (Internet Protocol) over a network that uses packet-switching technology. Since VoIP is based on computer systems it is vulnerable to security attacks in the same way as any other computer system. VoIP calls are

vulnerable to a variety of threats. Examples of these threats are spoofing, interception or eavesdropping, denial of service and spam over VoIP. Fig. 1 shows a typical VoIP network.

Main VoIP components in fig. 1 are:

a) IP PBX (Internet Protocol Private Branch eXchange) that switches calls between VoIP users on local lines and allow all users to share a certain number of external phone lines.
b) VoIP clients that use the IP PBX using IP, USB or soft phones
c) PSTN (public switched telephone network) for external calls

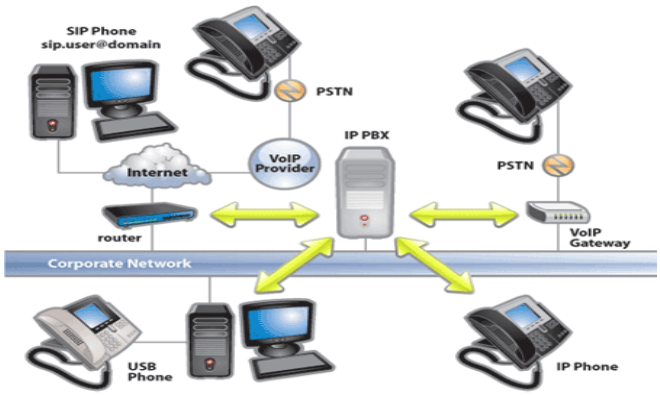

Fig. 1 VoIP Network [12]

VoIP Protocols

i. H.323

H.323 is the ITU (International Telecommunications Union) specification for audio and video communication across packetized networks.

An H.323 network is made up of several endpoints (terminals), a gateway, and possibly a gatekeeper, Multipoint control unit, and Back End Service. Fig. 2 shows H.323 architecture. The gatekeeper is often one of the main components in H.323 systems. It provides address resolution and bandwidth control. The gateway serves as a bridge between the H.323 network and the outside world of (possibly) non-H.323 devices. This includes SIP networks and traditional PSTN networks. [7]

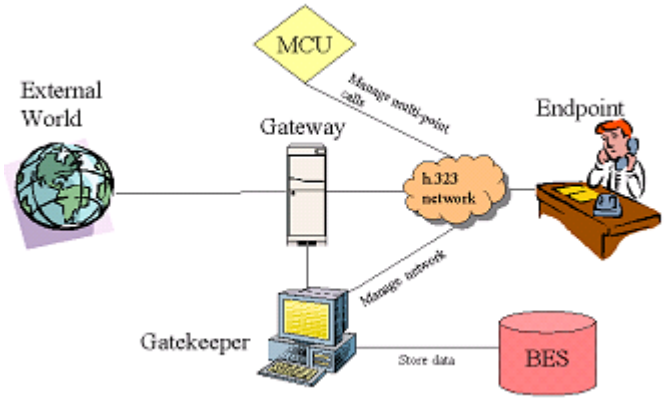

Fig. 2 H.323 Architecture [7]

ii. SIP (Session Initiation Protocol)

SIP is the IETF (Internet Engineering Task Force) specified protocol for initiating a two-way communication session. A SIP network is made up of end points, a proxy and/or redirect server, location server, and registrar. Fig. 3 shows SIP network architecture. In the SIP model, a user is not bound to a specific host. Initially the user reports their location to a registrar, which may be integrated into a proxy or redirect server. This information is stored in the external location server.

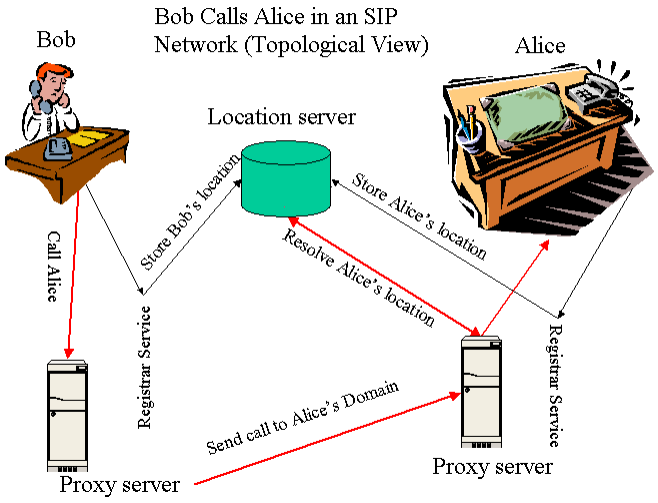

Fig. 3 SIP Network Architecture [7]

Messages from endpoints must be routed through either a proxy or redirect server. The proxy server intercepts messages from endpoints or other services, contacts the location server to

resolve the username into an address and forwards the message to the appropriate end point or another server.

SIP has a number of security mechanisms, Such as TLS, HTTP Digest, IPsec with IKE, manually keyed IPsec without IKE and S/MIME . [7]

Originally, VoIP traffic flows across the Internet in unencrypted packets, which means anyone that has access to the network between sender and recipient can intercept these packets and reveal their contents. Therefore, encryption should be used to hide such traffic flows and make them of no use to attackers.

Encryption is the process of converting a plaintext message into ciphertext which can be decoded back into the original message. An encryption algorithm along with a key is used in the encryption and decryption of data. There are several types of data encryptions which form the basis of network security. Encryption schemes are based on block or stream ciphers. [10]

The type and length of the keys utilized depend upon the encryption algorithm and the amount of security needed. In conventional symmetric encryption a single key is used. With this key, the sender can encrypt a message and a recipient can decrypt the message but the security of the key becomes problematic. In asymmetric encryption, the encryption key and the decryption key are different. One is a public key by which the sender can encrypt the message and the other is a private key by which a recipient can decrypt the message. [10]

III. SYSTEM PERFORMANCE

Performance is any characteristic of a software product that could be, in principle, measured by sitting at the computer with a stopwatch. The dimensions of performance include responsiveness (response time or throughput) and scalability.

A. VoIP performance

In ensuring the QoS for VoIP, researchers have come up with some QoS parameters as to be observed. Table I shows some of these parameters.

TABLE I :NETWORK QOS PARAMETERS

Category	Parameters
Timeliness	Delay Response time Jitter
Bandwidth	Systems-level data rate Application-level data rate Transaction time
Reliability	Mean time to failure (MTTF) Mean time to repair (MTTR) Mean time between failures (MTBF) Percentage of time available Packet loss rate Bit error rate

Three QoS parameters have been selected for VoIP performance measurement in this paper:

1. *End-to-end Delay:*

This is the delay for packet delivery from source to destination and is a general problem in all telecommunication networks.

2. *Jitter:*

Jitter is the variation in delay for packet delivery and occurs due to improper queuing and network congestion.

3. *Packet Loss:*

Packet loss occurs due to many factors but the usual cause is network congestion.

Table II below shows values for delay, jitter and packet loss recommended by the ITU (International Telecommunications Union) for performance from excellent to poor. [7]

TABLE III :ITU RECOMMENDED VALUES FOR VOIP QUALITY

Delay	< 150ms	>150ms < 300ms	>300ms
Jitter	< 20ms	> 20ms < 50ms	> 50ms
Packet Loss	< 1%	> 1% < 5 %	> 5 %
Performance	Excellent	Good	Poor

B. Encryption and Performance

Encryption algorithms apply cryptographic functions to the packets and introduce delay for the encryption and decryption of voice packets, the stronger the algorithm the greater the delay.

The studies performed by Barbieri et al. revealed the cryptographic engine as a bottleneck for voice traffic transmitted over IPSec. The driving factor in the degraded performance produced by the cryptography was the scheduling algorithms in the crypto-engine itself. However, there still was significant latency due to the actual encryption and decryption.

Barbieri et al. set up a controlled experiment to measure the effect of encryption and decryption on throughput. They tested four cryptographic algorithms on a fully VoIP dedicated network with a 100Mbps link (to negate saturation issues) using the same traffic in plain form as a benchmark. The algorithms tested were (in increasing order of computational expense) DES, 3DES, NULL (no encryption) + SHA-1, and 3DES + SHA-1. The results showed that the computationally lighter algorithms achieved better throughput than the more expensive ones. The disparities between each of the algorithms represent the relative latencies associated with the computational time for each algorithm. The range in throughput is significant, with a difference of approximately 500 packets per second between DES and 3DES + SHA-1 at a high traffic volume. Encryption/decryption latency is a problem for any cryptographic protocol, because much of it results from the computation time required by the underlying encryption. [8]

A number of protocols can be used to provide integrity, confidentiality and authentication of SIP signaling messages. These protocols include the use of IPSec, TLS, S/MIME, DTLS and HTTP digest authentication. The selection and adopting of the security protocol is normally dependant on the ease of use and scalability of the implementation. HTTP digest authentication is the simplest method where a message digest key or hash function is used as a digest authentication to protect the shared secret key during the SIP session negotiation. [4]

The IPSec protocol is widely used particularly in a SIP environment since it gives protection to applications that use UDP or TCP. It can be used in transport mode or in tunnel mode to secure the payload. The way that IPSec is used in this investigation is to create secure tunnels between the end devices in order to provide integrity, confidentiality and authentication for signaling and media messages. [4]

IV. EXPERIMENTAL SETUP

Experimental setup measures encryption impacts on VoIP network performance. We use IPX server with AES encryption algorithm as a security mechanism. Network analysis tool is used to measure the performance.

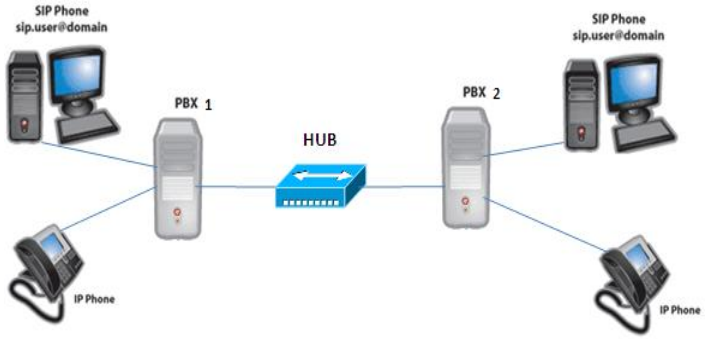

Fig. 4 Two PBXs connected with peer to peer topology

Fig. 4 shows the network topology we use. It contains two PBXs (Private Branch eXchange) which is the VoIP server, connected with a peer to peer topology using a hub. IP phones and soft phones are used for making calls between the PBXs. Wireshark is the network traffic analysis tool we use. Below is description about all these components.

1) VoIP server

Our VoIP server is PBX device designed by SIMTON Company. The VoIP software is developed by them. The operating system is Linux with kernel version 2.4. All configurations like server setup, network configuration and clients configuration, are done through web interfaces provided by SIMTON. They also provide customized AES encryption as security mechanism for VoIP calls.

2) Encryption algorithm

Encryption algorithm is a customized AES (Advanced Encryption Standard), as we mention. AES is a symmetric 128-bit block data encryption technique. It is customized by third party, and embedded in the PBX.

From the web based interface there are security options; disable, enable or customize. In the customize option AES can be used and managed.

AES is used for securing the PBX, because there is no evidence that AES has any weaknesses making any attack other than brute force possible (this is when the PBX is developed).

Signaling messages and data messages are both encrypted.

3) Network Tool

Wireshark is the tool used for analysis, formerly known as Ethereal. It is a network protocol analyzer. Its job is to listen to network traffic. We use it to measure VoIP QoS parameters namely delay, jitter and packet loss.

4) Soft phones and IP phones

After adding SIP accounts in the PBX server, we use soft phones and IP phones to use these accounts.

Soft phone is a computer application that allows users to make telephone calls directly from their computer. We use X-Lite soft phone. Fig. 5 below shows X-lite soft phone. IP phones used to make phone calls over an IP network, such as the Internet or an intranet.

The PBX has the ability to define 9 clients, 8 soft phones and 1 IP Phone.

Fig. 5 X-Lite Soft phone [16]

V. RESULTS

1. Delay

We calculate delay from the information provided by Wireshark. Results are in table III. In the insecure case AES encryption is disabled and SIP and RTP are not encrypted. The secure case signaling messages and data messages are encrypted using AES.

TABLE III :AVERAGE DELAY

	Average delay (ms)
Insecure	0,0009271
Secure	0,0095848

2. Jitter

Table IV shows jitter values provided by Wireshark.

TABLE IV :AVERAGE JITTER

	Average jitter (ms)
Insecure	19.1
Secure	30.4

3. Packet loss

Packet loss is less than 1% in both cases, secure and insecure.

VI. CONCLUSIONS

From measurements that presented in the previous section we notice that delay is increased by 9% approximately when using AES encryption. Jitter has also been affected by the encryption

and its performance is dropped by over 50% although it stays at the "Good" level. Considerable effects on packet loss have not been realized.

Based on discussions in this paper on the importance of encryption especially on the Internet, it is obvious that a compromise between high performance and high security needs to be reached. Further studies as of the most suitable encryption algorithms and techniques for VoIP systems have to be carried out and more performance parameters have to be included.

VII. REFERENCES

[1] Freescale Semiconductor, Nat Hillary, Measuring Performance for Real-Time Systems, 2005William Stallings, Cryptography and Network Security principles and Practices, 4th Edition

[2] A.H.Muhamad Amin, VoIP Performance Measurement Using QoS, The Second International Conference on Innovations in Information Technology (IIT'05)

[3] Vittorio Cortellessa1, Catia Trubiani1, Leonardo Mostarda2, and Naranker Dulay21 Universit`a degli Studi dell'Aquila, L'Aquila, Italy , An Architectural Framework for Analyzing Tradeoffs between Software Security and Performance, 2010

[4] Muhammad T. Asraf and John N. Davies, An Investigation into the Effect of Security on Performance in a VoIP Network, 11-1-2009

[5] Connie U. Smith and Lioyd G.Williams, Performance Solution: A practical guide for scalable responsive, scalable software, Learn basics and latest aspects of IT service management at CMG's annual conference

[6] Edward Paul Guillen, Diego Alejandro Chacon, VoIP Networks Performance Analysis with Encryption Systems, World Academy of Science, Engineering and Technology 58 2009

[7] D. Richard Kuhn, Thomas J. Walsh, Steffen Fries, Security Considerations for Voice Over IP Systems, Recommendations of the National Institute of Standards and Technology

[8] http://www.shrubbery.net/solaris9ab/SUNWaadm/SYSADV2/p71.html

[9] Aameek Singh Aameek , Sandeep Gopisetty and Linda Duyanovich, Security vs Performance: Tradeoffs using a Trust Framework , In Proceedings of the 22nd IEEE / 13th NASA Goddard Conference on Mass Storage Systems and Technologies, 2005

[10] Athina P. Markopoulou, Fouad A. Tobagi and Mansour J. Karam, Assessing the quality of voice communications over internet backbones, Journal IEEE/ACM Transactions on Networking (TON) archive , Volume 11 Issue 5, October 2003

[11] searchunifiedcommunications.techtarget.com, accessed at February 2011

[12] gdp.globus.org, accessed at February 2011

[13] http://www.linuxjournal.com/article/9398, accessed at February 2011

[14] http://searchunifiedcommunications.techtarget.com/definition/IP-PBX, accessed at September 2011